

FORM PTO-1390
(REV 12-29-99)

U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

ATTORNEY'S DOCKET NUMBER

GIL.P.US0017

TRANSMITTAL LETTER TO THE UNITED STATES
DESIGNATED/ELECTED OFFICE (DO/EO/US)
CONCERNING A FILING UNDER 35 U.S.C. 371

U.S. APPLICATION NO. (If known, see 37 CFR 1.5)

09/980731

INTERNATIONAL APPLICATION NO.
PCT/GB00/01354INTERNATIONAL FILING DATE
10 April 2000

PRIORITY DATE CLAIMED

2646 April 1999 BAC 2/21/02

TITLE OF INVENTION

MECHANISM FOR SECURING RELIABLE EVIDENCE FROM COMPUTERS AND LISTENING

APPLICANT(S) FOR DO/EO/US

DEVICES

ALISTAIR BRUCE KELMAN

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
 - a. ☒ is transmitted herewith (required only if not transmitted by the International Bureau).
 - b. ☐ has been transmitted by the International Bureau.
 - c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☐ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
 - a. ☒ are transmitted herewith (required only if not transmitted by the International Bureau).
 - b. ☐ have been transmitted by the International Bureau.
 - c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
 - d. ☐ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern document(s) or information included:

11. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☒ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A **FIRST** preliminary amendment.
☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
14. ☐ A substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☒ Other items or information:

Bibliographic Data Sheet

Copy of Filed International Application No. PCT/GB00/01354

with International Search Report

Postcard

Check in the amount of \$430.00

Transmittal Sheet

Copy of International Preliminary Examination Report

with Annex of Claims 1-9

17. ☒ The following fees are submitted:**BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)):**

Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO \$970.00

International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO \$840.00

International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO \$690.00

International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4) \$670.00

International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) \$96.00

ENTER APPROPRIATE BASIC FEE AMOUNT =**CALCULATIONS PTO USE ONLY**

\$ 860.00

Surcharge of \$130.00 for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).

\$

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE
Total claims	9 - 20 =	0	X \$18.00
Independent claims	3 - 3 =	0	X \$78.00

\$ 0

\$ 0

MULTIPLE DEPENDENT CLAIM(S) (if applicable)

+ \$260.00

\$

TOTAL OF ABOVE CALCULATIONS =

\$ 860.00

Reduction of 1/2 for filing by small entity, if applicable. A Small Entity Statement must also be filed (Note 37 CFR 1.9, 1.27, 1.28).

\$

430.00

SUBTOTAL =

\$ 430.00

Processing fee of \$130.00 for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)).

\$

+

TOTAL NATIONAL FEE =

\$

Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). \$40.00 per property

+

\$

TOTAL FEES ENCLOSED =

\$ 430.00

Amount to be
refunded: \$

charged: \$

a. ☒ A check in the amount of \$ 430.00 to cover the above fees is enclosed.b. ☐ Please charge my Deposit Account No. _____ in the amount of \$ _____ to cover the above fees. A duplicate copy of this sheet is enclosed.c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 18-0987. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Renner, Kenner et al.

First National Tower, 4th Floor

Akton, OH 44308

SIGNATURE:

NAME

Andrew B. Morton

REGISTRATION NUMBER

37,400

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

#3/10

In the application of

ALISTAIR BRUCE KELMAN


International App. No. PCT/GB00/01354

Internationally Filed 10 April 2000

For MECHANISM FOR SECURING RELIABLE
EVIDENCE FROM COMPUTERS AND
LISTENING DEVICES

**CERTIFICATE OF MAILING
VIA EXPRESS MAIL**

I hereby certify that this correspondence was deposited with the United States Postal Service as Express Mail, in an envelope addressed to: BOX PATENT APPLICATION, Assistant Commissioner for Patents, Washington, D.C. 20231, on October 25, 2001.


Faye Leppla, Secretary to Andrew B. Morton
Express Mail Label No. EL725989885US

PRELIMINARY AMENDMENT

Box PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.D. 20231

Sir:

The Applicant, through his attorney, requests that the following amendments be entered prior to examination and prior to calculation of the filing fee. For clarification, the Applicant acknowledges that the claims which are being amended are based upon the claims as filed in the International Application and as amended in the International Preliminary Examination Report.

In the claims:

Please amend claims 1-9 as follows:

1. A device for use in validating recorded digitized information including voice, video, telemetry or computer generated information or the like, characterised in that the device includes a tamper-proof unit accommodating means for identifying the date and time and serial number of the device in a cipher data register and the private key of a public/private key encryption pair allocated to the device, the device being arranged in operation to produce a data file for recording on standard recording media having a header and an enciphered message, the recorded message being enciphered by a cipher unit with the date,

time and serial number held in the said cipher data register and the header contains the private key encrypted date, time and serial number used in the cipher process provided by an encryption unit, the device further including a geophysical location defining unit for generating geophysical location information indicative of the actual location of the device and said geophysical location information is used by the cipher unit to encipher the recorded message and is included by the encryption unit in the encrypted header.

2. A device as claimed in claim 1 in which the geophysical location defining unit is a digital mobile telephone instrument of the type including a global positioning system.
3. A device as claimed in claim 2 in which the mobile telephone instrument includes a short message service system and every encrypted header is also sent to a trusted third party by way of the mobile telephone short message service system.
4. A device as claimed in claim 1 in which the encryption unit also creates a digital fingerprint for incorporation in the header which said digital fingerprint comprises a unique value calculated from the message.
5. A device as claimed in claim 1 in which an inbuilt location identifier is programmed with the actual geophysical location of the device and is arranged to inhibit the operation of the cipher unit and the encryption unit if the values of the actual geophysical location identifier and the geophysical location information generated by the geophysical unit do not equate.
6. A process for use in validating recorded digitized voice, video, telemetry or digital computer generated information, characterised in that the process produces a data file of the recorded information enciphered with the date, time and serial number of the recording equipment and forms a file header containing the date, time and serial number used in the enciphering process encrypted with the private key of a public/private key pair, wherein the recorded information is also enciphered with geophysical location information which is also formed in to the file header.

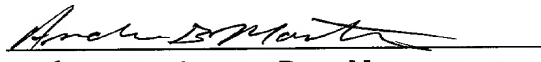
- 09980731-103501
7. A process as claimed in claim 6 in which the file header is sent to a trusted third party to validate enciphered recorded information and encrypted header.
 8. A process as claimed in claim 6 in which the header also incorporates a digital fingerprint comprising a unique value calculated from the message.
 9. A copyright management system for use with an electronically distributed digital product which management system employs a set-top box which includes means for generating an encrypted message arranged at the end of a download by the set top box to create an encrypted message including the private key encrypted date, time, serial number and geophysical location of the set top box together with an identification code of the work downloaded for communication over the short message service system of a mobile telephone system to a distributor of the electronic digital product.

REMARKS

The amendments presented hereinabove have been made in order to eliminate multiple dependencies on some of the claims. Additionally, initialisms that refer to some of the elements have also been removed. As these amendments do not add new subject matter, it is respectfully requested that they be entered. Upon entering the amendments, claims 1-9 will now be pending.

Should the Examiner care to discuss any of the foregoing in greater detail, the undersigned attorney would welcome a telephone call.

Respectfully Submitted,


Andrew B. Morton, Reg. No. 37,400
Rodney L. Skoglund, Reg. No. 36,010
Renner, Kenner, Greive, Bobak,
Taylor & Weber
First National Tower, 4th Floor
Akron, Ohio 44308-1456
Telephone: (330) 376-1242
Attorney for Applicant

October 25, 2001

Marked-Up Version of the Claims
International Application No. PCT/GB00/01354

1. A device for use in validating recorded digitized information including voice, video, telemetry or computer generated information or the like, characterised in that the device includes a tamper-proof [(TPB)]unit accommodating means for identifying the date and time [(RTC)] and serial number of the device [(SRN)] in a cipher data register [(CDR)] and the private key [(PCR)] of a public/private key encryption pair allocated to the device, the device being arranged in operation to produce a data file for recording on standard recording media [(RD)] having a header [(H-Data)] and an enciphered message [(DATA)], the recorded message being enciphered by a cipher unit [(CU)] with the date, time and serial number held in the said cipher data register [(CDR)]and the header [(H-Data)]contains the private key encrypted date, time and serial number used in the cipher process provided by an encryption unit [(EU)], [and characterised in that] the device further [includes] including a geophysical location defining unit [(GU)] for generating geophysical location information [(C)] indicative of the actual location of the device and said geophysical location information is used by the cipher unit [(CU)] to encipher the recorded message and is included by the encryption unit [(EU)] in the encrypted header [(H-Data)].
2. A device as claimed in claim 1 in which the geophysical location defining unit [(GU)] is a digital mobile telephone instrument of the type including a global positioning system.
3. A device as claimed in claim 2 in which the mobile telephone instrument [(GU)] includes a short message service system and every encrypted header [(H-Data)] is also sent to a trusted third party by way of the mobile telephone short message service system.
4. A device as claimed in [any preceding claim] claim 1 in which the encryption unit [(EU)] also creates a digital fingerprint for incorporation in the header [(H-Data)]

09980731-1099901

[comprising] which said digital fingerprint comprises a unique value calculated from the message.

5. A device as claimed in [any preceding claim] claim 1 in which an inbuilt location identifier [(LI)] is programmed with the actual geophysical location [(PL)] of the device and is arranged to inhibit the operation of the cipher unit [(CU)] and the encryption unit [(EU)] if the values of the actual geophysical location identifier [(LI)] and the geophysical location information [(C)] generated by the geophysical [(GU)] unit do not equate.
6. A process for use in validating recorded digitized voice, video, telemetry or digital computer generated information [or the like], characterised in that the process produces a data file of the recorded information enciphered with the date, time and serial number of the recording equipment and forms a file header [(H-Data)] containing the [private key encrypted] date, time and serial number used in the enciphering process encrypted with the private key of a public/private key pair, [and characterised in that] wherein the recorded information is also enciphered with geophysical location information which is also formed in to the file header [(H-Data)].
7. A process as claimed in claim 6 in which the file header [(H-Data)] is sent to a trusted third party to validate enciphered recorded information and encrypted header.
8. A process as claimed in claim 6 [or claim 7] in which the header also incorporates a digital fingerprint comprising a unique value calculated from the message.
9. A copyright management system for use with an electronically distributed digital [products such as music, video and multi-media works, characterised in that an electronic distribution system includes] product which management system employs a set-top box which includes means for generating an encrypted message arranged at the end of a download by the set top box to create an encrypted

message including the private key encrypted date, time, serial number and geophysical location of the set top box together with an identification code of the work downloaded for communication over the short message service system [(SMS)] of a mobile telephone system to a distributor of the electronic digital product [(distributor)].

09580731 403804

09/980731

JC13 Rec'd PCT/PTO 25 OCT 2001
PCT/GB00/01354

WO 00/65771

Title:

1/pst

Mechanism for securing reliable evidence from computers and listening devices

Technical Field

This invention relates to methods and apparatus for securing and preserving evidence from computers and listening devices in a form which eliminates or reduces the need for corroborative or supporting evidence regarding the circumstances of the making of the recording.

Background

Throughout the history of computing it has been known that evidence from computers has been modifiable in most cases without trace. Modification and fabrication of computer evidence has led to serious problems in the investigation and prosecution of computer crimes, in the management of computer security, in the keeping of business records in accordance with the security provisions of the Companies Acts and in the cost of litigation where evidence has been derived from computers.

In criminal investigations the reliability of evidence from computers has had to be secured by complex administrative procedures ("bagging and tagging") when freezing computer evidence at the scene of an alleged crime together with the use of image copying equipment to take bit image copies of suspected computer systems. Police officers and computer staff have had to give detailed evidence regarding how they secured computer systems and preserved the computer evidence. In managing computer security there have been cases where it has been difficult or impossible to show precisely what data or programs were on particular computer systems at particular times. In the keeping of business records there have concerns about the conversion of paper records into document image copies and their subsequent reliability as contemporaneous evidence. One security concern has been the fact that a document image copy can be used to create modified versions of itself which cannot be

09980731-10501

WO 00/65771

PCT/G800/01354

- 2 -

shown to be forgeries without a very expensive forensic examination being undertaken - and sometimes with it being impossible to prove that the document image is an unmodified original. Consequently expensive administrative controls regarding the storage of document image copies are necessary to maintain adequate security.

Additionally police and security services have made greater use of listening devices under warrant for the monitoring of suspected criminals. Currently under UK legislation the evidence from such listening devices can only be used for intelligence gathering purposes and cannot be tendered in evidence in civil or criminal trials. This situation is presently under review and it is anticipated that UK law will be changed to allow for evidence from listening devices under warrant to be admissible in civil and criminal trials in certain circumstances. Concern has been expressed regarding the need for security services personnel to testify regarding the planting of listening devices and their compliance with administrative procedures to secure the reliability of evidence from listening devices.

Object of the Invention

It is an object of the invention to provide a computer peripheral, termed the "DataFreeze", which will automatically secure evidence in a form which will be accepted as being electronically "bagged and tagged" - that is to say the evidence will be encapsulated in a form which establishes precisely when it was obtained and where it was obtained.

According to the invention there is provided a device for use in validating recorded digitised voice, video, telemetry or computer generated information or the like, characterised in that the device includes a tamper-proof unit accommodating means for identifying the date, time and serial number of the device and the private key of a Public key encryption pair allocated to the device, the device being arranged in operation to produce a data file for recording on recording media having a header and an enciphered message, the recorded message being enciphered with the date, time and

09980731-102501

WO 00/65771

PCT/GB00/01354

- 3 -

serial number of the device and the header containing the private key encrypted date, time and serial number used in the cipher process.

According to the invention there is provided a process for use in validating recorded digitised voice, video, telemetry or digital computer generated information or the like, in which the process produces a data file of the recorded information enciphered with the date, time and serial number of the recording equipment and forms a file header containing the private key encrypted date, time and serial number used in the enciphering process.

According to a feature of the invention the cipher process and encrypted header also include geophysical location information indicative of the actual location of the device making the validated recording.

The device according to the invention may be a micro-processor controlled arrangement and the process of the invention may be performed by a computer program.

The equipment of the invention performs these operations in real-time without adding any significant delay to the recording of the data, without the need for a powerful encryption microprocessor and without the need for skilled personnel. Once the recording has been secured and encapsulated by the DataFreeze hardware the resulting disk, tape, electronic recording, magnetic recording or optical recording is re-playable on any conventional replay device for the replay of that type of media running special DataFreeze deciphering software. Consequently, in one possible implementation, a prosecuting authority could supply to an accused's lawyers with a CDROM produced by the arresting officers on a DataFreeze peripheral which was readable by the accused's lawyers on their conventional windows personal computer with the DataFreeze decryption/deciphering software running. No additional hardware would be required by the defence lawyers. The date, time, geophysical or CURSOR location and serial number of the DataFreeze peripheral used to make the recording would

0950734 10594

WO 00/65771

- 4 -

PCT/GB00/01354

however always be available to the defence in confirmation of when, where and on what equipment the data had been frozen by the police or security forces.

Outside of the police and security services a DataFreeze peripheral could be used as an archival storage device in banking and financial services or as a tachograph or other work monitoring device in medical and in health and safety applications.

Description of one embodiment of the invention

One embodiment of the invention will be described with reference to the accompanying drawing.

The manufacturer, DataFreeze, generates a Public Key encryption pair for each unit to be manufactured - the public key being published as an X500 Digital Certificate and the private key being kept secret. Each private key is built into a private key register PCR on a custom chip in a tamper-proof module TPB. Inside a DataFreeze peripheral is the custom chip in a tamper-proof module TPB which is connected to a standard recording device RD (e.g. A CDROM writer or a floppy disk drive). The custom chip embodies a micro-processor and contains a geophysical positioning system GU (in one implementation of the invention a CURSOR mobile telephone positioning system), a real-time clock RTC and a unique serial number SRN. The output from these three devices, in one possible implementation, is converted into a 512 bit number with the left portion containing the data and time D, the middle containing the positioning system's location (the CURSOR location) C and the right portion containing the Serial Number S in a cipher data register CDR.

Within the custom chip the 512 bit number in the cipher data register CDR is encrypted using the private key from the private key register PCR of the particular unit in the encryption unit EU. The resulting encrypted stream is called "H-Data". Because the volume of data (512 bits) being encrypted by the private key is very small, the vulnerability of the data to cryptanalysis to discover the private key is very low.

009980731-102501

WO 00/65771

PCT/GB00/01354

- 5 -

To start a recording session the DataFreeze unit receives data from an external source LS (line under Surveillance) (e.g. a computer or a listening device). The DataFreeze unit notes the "H-Data" and writes this to the recording media RD as a header to the recording, padding any spare space in the header with zeros.

The DataFreeze unit now takes the first block of data received from the external source stored in the cipher unit CU. It performs three simple Caesar cipher operations on the block of data e.g. Multiplying the block of data by the new date and time and adding the cursor location and the square of the serial number.

$$\text{i.e. DataFreeze block} = ([\text{Data}] * D1) + C + (S * S)$$

For the next block of data it performs a different calculation e.g. Multiplying the block of data by the CURSOR location, adding the square of the new date and time (which will have increased a defined amount during the writing of the first block) and adding the serial number.

$$\text{i.e. DataFreeze block} = ([\text{Data}] * C) + (D2 * D2) + S$$

For the next block of data it performs a different calculation e.g. Multiplying the block of data by the square of the serial number, adding the square of the CURSOR location and adding the new date and time (which will have increased a defined amount during the writing of the second block).

$$\text{i.e. DataFreeze block} = ([\text{Data}] * S * S) + D3 + C$$

For the fourth block of data the DataFreeze peripheral would revert to enciphering using the algorithm used for the first block of data.

$$\text{i.e. DataFreeze block} = ([\text{Data}] * D4) + C + S$$

Further variations on this manipulation are possible. However particular care must be taken in selection of the manipulations to avoid floating point operations which are

00930731-102501

WO 00/65771

PCT/GB00/01354

- 6 -

likely to introduce floating point precision errors in the calculation when this is performed on conventional microprocessors.

The objective of the DataFreeze enciphering is not to make the data cryptographically secure i.e. secret. Rather it is to freeze the data as recorded with the date and time when it was recorded, the location where it was recorded and the unit on which it was recorded. For proof of no tampering it has to do this in real-time. The simple manipulations of data are performed in a few cycles of the microprocessor running on the DataFreeze peripheral and cause no material delay in the writing of the data.

To replay a DataFreeze recording on a standard replay device the computer controlling the device would run the DataFreeze decryption/deciphering software. This would read the "H-data" from the header and decrypt it using the DataFreeze public key, which would be published as an X500 digital certificate. Once the header had been decrypted the left, middle and right portions of the header would be stored in buffers and used as the seed data for a computer program to step through the obverse of the enciphering process. Thus in the suggested implementation - the first block of DataFreeze data would have the CURSOR location subtracted and the square of the serial number subtracted with the result being divided by the date and time.

$$\text{i.e. Data} = ([\text{DataFreeze Data}] - C - (S^2))/D1$$

The second block of DataFreeze data would have the square of the new date and time (which will have increased a defined amount during the writing of the first block) subtracted, the serial number subtracted and the result divided by the CURSOR location.

$$\text{i.e. Data} = ([\text{DataFreeze Data}] - D2 - S)/C$$

The third block of data would have the square of the CURSOR location subtracted, the new date and time (which will have increased a defined amount during the writing

09980731.105501

WO 00/65771

PCT/GB00/01354

- 7 -

of the second block) subtracted and the result divided by the square of the serial number.

$$\text{i.e. Data} = ([\text{DataFreeze Data}] - (C * C) - D3) / (S * S)$$

Such simple mathematical processes would not lead to any material overhead in the outputting of the data. It would also be possible to 'fast forward' and 'reverse' along a DataFreeze recording by noting the block number from the header and cycling through to the predicted algorithm, date and time, CURSOR location and serial number.

With sufficient computing power and time it would always be possible to decipher a DataFreeze recording which had lost its header by trying various combinations of date, location and serial number against the fragment of the recording. However because the H-Data is digitally signed using the private key of the DataFreeze X500 digital certificate of the particular unit and the private key is located within a tamper proof module within the CURSOR unit along with the real time clock it would not be possible to create a fabricated DataFreeze recording which predated the original since this would require the forgery of the cryptographically secure H-data in the header.

A more sophisticated version of the invention could include a "digital fingerprint" in the header along with the H-Data. This would be produced by simultaneously passing a duplicate of the entire data session through a one-way algorithm while it was being written to disk to produce a unique value known as a message digest which would, in effect, be a "digital fingerprint" of the session. This message digest could then be encrypted by the DataFreeze unit's private key and written to the header field H-data of the recording. When decrypted in software by using the DataFreeze unit's X500 public key this message digest could be used to confirm the integrity and coherence of the recording of the data session.

A further version of the invention could contain a dummy or non-functional CURSOR unit located in the tamper-proof module. This would not determine the location of the

09980731 "105501"

WO 00/65771

PCT/GB00/01354

- 8 -

unit but would simply give out a default location for inclusion in the H-Data. The DataFreeze unit would thus only stamp the data with the time and specific unit and the default location. Such a unit would have two main uses: Use in situations where it was not possible to get a location signal and use in situations where the cost of the DataFreeze unit needed to be low and the location information was not considered to be important.

In yet a further version of the invention the geophysical information may be used to control the use of the recording equipment by having an inbuilt location identifier LI which is programmable (i.e. lead PL is set with the geophysical location of the device) and is used to prevent use of the recording equipment if it is located outside the geophysical area indicated by the inbuilt location identifier LI by inhibiting the cipher unit CU and encryption unit EU if the values of PL and C do not equate. Typically the geophysical positioning unit may be the Global positioning system used in mobile telephones by including a complete mobile telephone instrument in the Position Unit GU.

Preferably the standard recording medium is of the "Write once read many times" type where it is impossible to purge a record once it has been written. However, the invention may be used with erasable media.

To overcome the security vulnerability of erasable media it is necessary to have a mechanism that detects deletions from the stored information. To ensure that such a deletion is detectable it is possible to arrange that the encrypted header H-data produced by the encryption unit EU of every document stored using DataFreeze is sent using the mobile cellphone incorporated into the position unit GU supplying the location information using a Short Message Service SMS message. This would provide an audit trail logged by a Trusted Third Party which could be compared with the electronic copy. If a document were purged on the erasable media its omission

09980731 102501
T0520T T08866

WO 00/65771

PCT/GB00/01354

- 9 -

would be obvious since the two sets of records, the SMS logs and the encrypted headers on the local copy would not be identical.

The invention has application beyond that involving criminal investigation. For example in the publishing industry copyright rights are traditionally allocated by physical territories. Thus a copyright owner can license one publisher to publish his work in a specific territory (e.g. USA) and another publisher to publish his work in a different territory (e.g. Europe) each paying different royalties. The ability to segregate territories is important for copyright owners to maximise their income through taking account of the relative wealth of particular territories. Thus the author of a book on soil science might reasonably wish to sell his book at \$15 a copy to people living in a wealthy country (E.g. USA) and at \$0.50 per copy to people living in a poor country (e.g. Cambodia) and make the material available free to a charitable foundation. An enhancement of the DataFreeze technology makes such a segregation possible.

In this implementation the DataFreeze unit according to the invention becomes part of a media recording device (e.g. a set top box supplied by a media company). Under this amended system the SMS message transmitted would consist of five parts: the normal encrypted DataFreeze header (with check sum to prove that the recording was complete); the ISBN (or equivalent) of the downloaded work (thereby identifying the work), the Location Information, the serial number of the set-top box and the date & time of download. These five parts would be encrypted using the public key of the set-top box maker.

By way of example instead of using a book we will consider the downloading of a pay-per-view music video. The consumer wishing to download the pay-per-view music video would instruct his unit to download it. At the end of the download the set-top box would send the encrypted SMS message to the media company. This message would be stored and from time to time (e.g. daily, weekly or monthly) the batches of

09980731.100001

WO 00/65771

PCT/GB00/01354

- 10 -

SMS messages would be decrypted using the private key of the media company thereby generating the DataFreeze header (proving that the material was successfully downloaded), the ISDN number (identifying the work downloaded), the Location Information (therefore establishing the territory in which the work was downloaded and consequently the amount of royalties due as well as the duty and consumption taxation due on the transaction), the serial number of the set-box (thereby establishing who to send the bill to) and the data and time of download (thereby establishing the period for billing purposes and also essential as billing information when the price due for the download varies over time).

Based upon the SMS data received the consumer would be sent (or directly debited) with his bill for the materials downloaded by his set-box and the media company would be able to account to the copyright owner and the national government for royalties, duty and taxes due for downloading in the territory where the set-top box was located. So if the set top box was registered to a charity in a specific location it would be possible for the bills to be waived.

One very specific advantage of this kind of system is that it contains within it protection against piracy. Any person using a DataFreeze set-top box for downloading would be identifying their physical location, necessary for the proper accounting of royalty payments, duty and taxes. If a set-top box was stolen the consumer would report the loss to the media company. Any download which occurred thereafter would give the new location of the stolen box, thereby assisting in the arrest and prosecution of the thief. Because the SMS message is encrypted using the private key of the media company, so long as this private key remains secure, there is no means by which the location information, the ISBN and the serial number of the unit could be falsified. However like all digital signature systems the security of the rights management system depends upon the private key being kept secret - consequently the company which generates and supplies the media company with its private and public key pair must be as trustworthy as a bank note supplier to governments.

09580731-105501

WO 00/65771

PCT/GB90/01354

- 11 -

One further variant on all forms of the DataFreeze unit according to the invention could have a biometric sensor attached to the unit. In this enhancement when a recording were to be made the biometric sensor would check the relevant biometric of the user (e.g. the fingerprint). If it found this to be valid it would then encrypt the DataFreeze header data with the private key associated with the user. This re-encrypted DataFreeze header would be written to the unit and, in an enhanced version, sent by SMS to the external store for audit purposes.

In this variant the decryption process has one further stage. Before commencing to decrypt the DataFreeze header encrypted in the way set out the original patent application the DataFreeze software would have to obtain the public key associated with the user. Using this public key it would decrypt the message to reveal the original encrypted DataFreeze header. Using the public key of the recording device the unit would then decrypt the DataFreeze header itself revealing the date, location, serial number (and checksum).

Both the user's public keys and the recording devices public keys could be obtained from a web site. In this implementation a further header could precede the DataFreeze header on the recording giving the URLs of the public key of the user and the public key of the recording device. In regular use this information could be downloaded and cached so that no material delay would occur when reading records produced by people or devices in frequent correspondence with each other.

All of the enhancements and variations identified above can be implemented by a suitably programmed micro-processor.

09980731-102501

CLAIMS

1. A device for use in validating recorded digitized information including voice, video, telemetry or computer generated information or the like, characterised in that the device includes a tamper-proof unit (TPB) accommodating means for identifying the date and time (RTC) and serial number of the device (SRN) in a cipher data register (CDR) and the private key (PCR) of a public key encryption pair allocated to the device, the device being arranged in operation to produce a data file for recording on standard recording media (RD) having a header (H-Data) and an enciphered message (DATA), the recorded message being enciphered by a cipher unit (CU) with the date, time and serial number held in the said cipher register (CDR) and the header (H-Data) contains the private key encrypted date, time and serial number used in the cipher process provided by an encryption unit (EU), and characterised in that the device includes a geophysical location defining unit (GU) for generating geophysical location information (C) indicative of the actual location of the device and said geophysical location information is used by the cipher unit (CU) to encipher the recorded message and is included by the encryption unit (EU) in the encrypted header (H-Data).

2. A device as claimed in claim 1 in which the geophysical location defining unit (GU) is a digital mobile telephone instrument of the type including a global positioning system.
3. A device as claimed in claim 2 in which the mobile telephone instrument (GU) includes a short message service system and every encrypted header (H-Data) is also sent to a trusted third party by way of the mobile telephone short message service.
4. A device as claimed in any preceding claim in which the encryption unit (EU) also creates a digital fingerprint for incorporation in the header (H-Data) comprising a unique value calculated from the message.
5. A device as claimed in any preceding claim in which an Inbuilt location Identifier (LI) is programmed with the actual geophysical location (PL) of the device and is arranged to inhibit the operation of the cipher unit (CU) and the encryption unit (EU) if the values of the actual geophysical location identifier (LI) and the geophysical location information (C) generated by the geophysical unit (GU) do not equate.

6. A process for use in validating recorded digitized voice, video, telemetry or digital computer generated information or the like, characterised in that the process produces a data file of the recorded information enciphered with the date, time and serial number of the recording equipment and forms a file header (H-Data) containing the private key encrypted date, time and serial number used in the enciphering process, and characterised in that the recorded information is also enciphered with geophysical location information which is also formed into the file header (H-Data).
7. A process as claimed in claim 6 in which the file header (H-Data) is sent to a trusted third party to validate enciphered recorded information and encrypted header.
8. A process as claimed in claim 6 or claim 7 in which the header also incorporates a digital fingerprint comprising a unique value calculated from the message.
9. A copyright management system for use with electronically distributed digital products such as music, video and multi-media works, characterised in that an electronic distribution system includes a set-top box which includes means for generating an encrypted message arranged at the end of a download by

08-05-2001

GB 000001354

15

the set top box to create an encrypted message including the private key encrypted date, time, serial number and geophysical location of the set top box together with identification code of the work downloaded for communication over the short message system (SMS) of a mobile telephone system to the electronic digital product distributor.

00980791-10501

Empfangszeit 8.Mai. 14:37

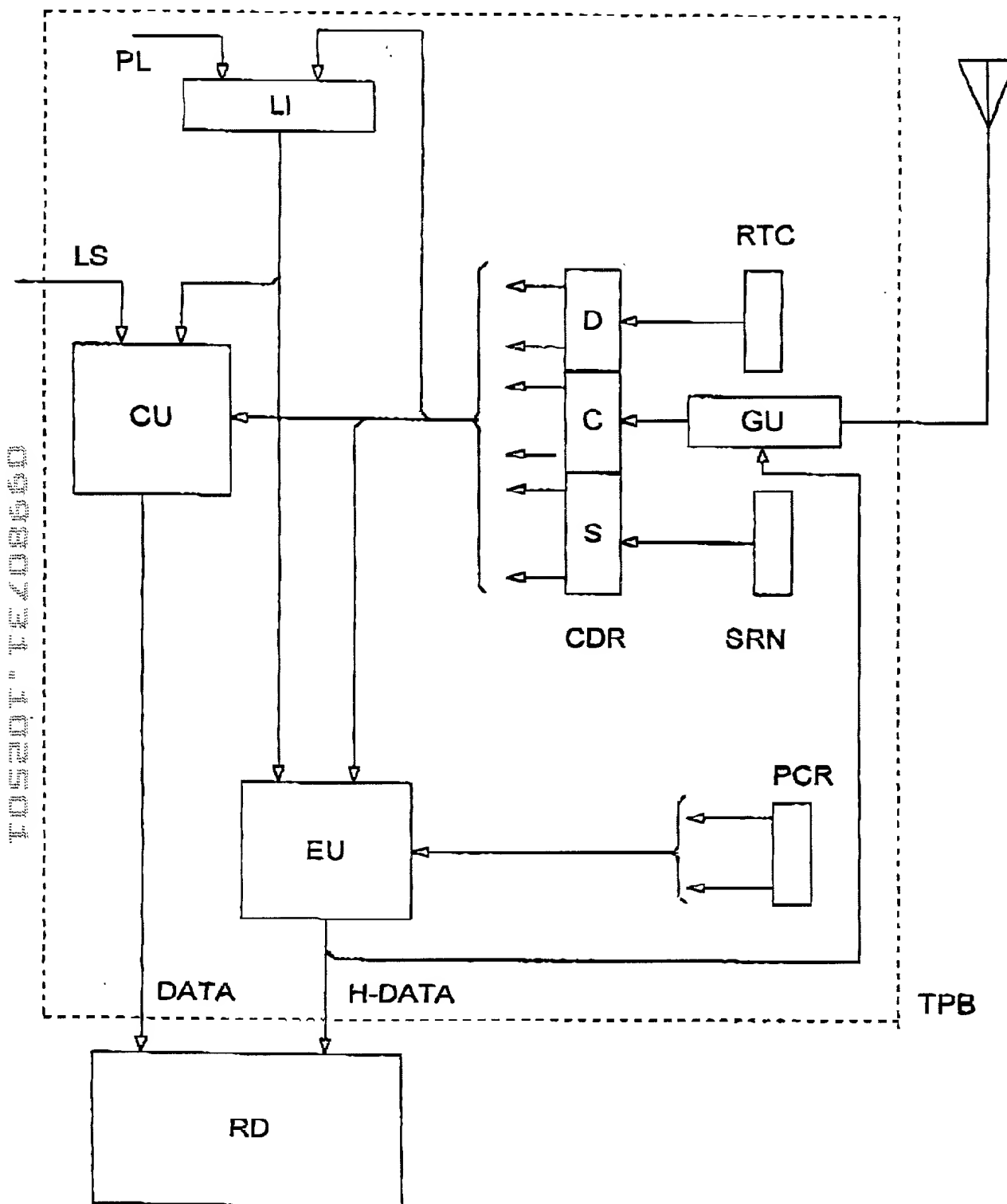
AMENDED SHEET

09/980731

WO 00/65771

PCT/GB00/01354

1/1



COMBINED DECLARATION AND POWER OF ATTORNEY

As the below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled
MECHANISM FOR SECURING RELIABLE EVIDENCE FROM COMPUTERS AND LISTENING DEVICES

the specification of which

_____ is attached hereto.

_____ was filed on _____ as Application Serial No. _____ and was amended on _____.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, ' 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, ' 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Priority Claimed

99 09590.3	Great Britain	26th April 1999	X	
Number	Country	Date Filed	Yes	No
PCT/GB00/01354	PCT	10th April 2000	X	
Number	Country	Date Filed	Yes	No

English Language Declaration

I hereby claim the benefit under Title 35, United States Code, ' 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this

application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, ' 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, ' 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

PCT/GB00/01354

10th April 2000

Application Ser. No.

Filing Date

Status

Application Ser. No.

Filing Date

Status

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith:

Reese Taylor (Reg. No. 22,325); Phillip L. Kenner (Reg. No. 22,353); Edward G. Greive (Reg. No. 24,726); Donald J. Bobak (Reg. No. 27,182); Ray L. Weber (Reg. No. 26,519); Joseph G. Curatolo (Reg. No. 28,837); Rodney L. Skoglund (Reg. No. 36,010); Andrew B. Morton (Reg. No. 37,400); Arthur M. Reginelli (Reg. No. 40,139); Salvatore A. Sidoti (Reg. No. 43,921); John J. Cunniff (Reg. No. 42,451); and Mark Weber (Reg. No. 46,069)

Send Correspondence to:

Rodney L. Skoglund
Renner, Kenner, Greive, Bobak, Taylor & Weber
First National Tower, 4th Floor
Akron, Ohio 44308


Direct Telephone Calls to:

Rodney L. Skoglund
Telephone: (330) 376-1242

DECLARATION

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereof.

SIGNATURE

Inventor: 
(Alistair Bruce KELMAN)
Name:

Date 16th Oct. 2001.

Residence:

37 Station Road, London NW4 4PN, GB *GBN*
(address)

Post Office Address:

(same as above)

Citizenship:

British
(country)